PRIVACY IMPACT ASSESSMENT (PIA)

For the

Total Army Injury and Health Outcomes Database (TAIHOD)
US Army Medical Command - DHP Funded System

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☐ New DoD Information System
- ☐ New Electronic Collection
- ☐ Existing DoD Information System
- ☒ Existing Electronic Collection
- ☐ Significantly Modified DoD Information System

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☐ Yes, DITPR — Enter DITPR System Identification Number
- ☐ Yes, SIPRNET — Enter SIPRNET Identification Number
- ☒ No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☐ Yes
- ☒ No

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

- ☐ Yes
- ☒ No

If "Yes," enter Privacy Act SORN Identifier

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

USC Title 10 Subtitle B Part I Chapter 303 § 3013, Secretary of the Army
SORN A0070-45 DASG, Medical Scientific Research Data Files (April 4, 2003, 68 FR 16484)
Army Regulation 40-5, Medical Services Preventive Medicine
Department of Defense Directive 3202.1, Use of Department of Defense Research Facilities by Academic Investigators
Department of Defense Instruction 3201.01, Management of DoD Research and Development Laboratories

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

Purpose: The purpose of the TAIHOD is to enable epidemiologic research on active duty Army with the specific goal of conducting research to improve and sustain Warfighter health and performance.

Personal information collected in the system: The following personal information is included: social security number (SSN), demographics (e.g., sex, date of birth), occupational (e.g., military occupational specialty, rank, pay), and clinical/health-related (e.g., date/type of clinical services received, disability evaluation/ discharge information).

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The risks associated with the PII collected are unauthorized access, unauthorized disclosure, and inaccurate information. Unauthorized access is safeguarded by 1) the TAIHOD being on an internal network not connected to any other network or the internet, and 2) requiring background checking and other vetting procedures on individuals prior to issuing them an account on the TAIHOD. Unauthorized disclosure is safeguarded by requiring all individuals with TAIHOD access to sign a confidentiality agreement, as well as other legally binding documents indicating that the individual will follow TAIHOD and US Army Institute of Environmental Medicine (USARIEM) policies in terms of disclosure. Individuals with TAIHOD access are also required to complete training on the handling of personal information. Having inaccurate information is safeguarded by having a professional Database Manager oversee the acquisition of data from the source agencies and facilitate its processing into the TAIHOD.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☐ **Within the DoD Component.**

Specify.

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

Name of contractor: Social Sectors Development Strategies, Inc.
Language in contract:
"Access to data from the TAIHOD shall be in accordance with the Federal Information Security Management Act (FISMA), the Privacy Act, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 109-461, §5725, Confidentiality of Drug Abuse, Alcoholism and Alcohol Abuse, HIV Infection and Sickle Cell Anemia Medical Records, 38 U.S.C. 7332, Confidentiality of Healthcare

Quality Assurance Review Records, 38 U.S.C. 5705. In addition, all actions of Contractors must be compliant with the Total Army Injury and Health Outcomes Database Standard Operating Procedure, H07-08, as well as all USARIEM policies and regulations, including those set forth by the USARIEM Human Research Protection Program. Contractor access to TAIHOD data, information and information systems must provide the highest level of protection possible from unauthorized disclosure of sensitive information, as held forth in the TAIHOD Confidentiality Agreement. TAIHOD datasets must be protected at the highest level of protection possible, regardless of whether they are residing on the TAIHOD network or have been transferred to the Contractor.

The TAIHOD SOP describes the expectations for Contractor data stewardship, including data acquisition and/or access, storage, use, transfer, and destruction. Contractor data stewardship must be in compliance with applicable Federal Information Processing Standards (FIPS) and Special Publications (SP) issued by the National Institute of Standards and Technology (NIST) concerning the TAIHOD information and data that are subject of this contract. It is the Contractor's responsibility to follow these policies with respect to the use of TAIHOD data. The Contractor is not at liberty to disclose data or information from the TAIHOD; any disclosure must be done only after an appropriate USARIEM approval process as stipulated in USARIEM policies.

Contractor shall provide access to TAIHOD data only to employees, subcontractors, and affiliates only: (1) to the extent necessary to perform the services specified in this Contract, (2) to perform necessary maintenance functions for electronic storage or transmission of media necessary to perform the contract, and (3) only to individuals who first satisfy the same conditions, requirements and restrictions that comparable USARIEM employees must meet in order to have access to the same TAIHOD data. These restrictions include the same level of background investigations, where applicable. These restrictions also include those described in the TAIHOD Confidentiality Agreement. The Contractor shall utilize only employees, subcontractors, or agents who are physically located within a jurisdiction subject to the laws of the United States.

The Contractor shall inform USARIEM (through informing the TAIHOD Director and IASO) by the most expeditious method available to the Contractor of any incident of suspected or actual access to, disclosure, disposition, alteration, or destruction of TAIHOD data or information not authorized under this Contract ("incident") within one hour of learning of the incident. The Contractor agrees to comply with directions provided by USARIEM to address the incident. To the extent practicable, Contractor shall mitigate any harmful effect on individuals whose TAIHOD data or information was accessed or disclosed in the incident.

The Contractor shall not publish or disclose in any manner the details of any safeguards either designed or developed by the Contractor under this contract, or otherwise provided by USARIEM.

USARIEM has the right during normal business hours to inspect the Contractor's facility, information technology systems and storage and transmission equipment, and software utilized to perform the contract to ensure that the Contractor is providing for the confidentiality and security of TAIHOD data and computer systems in accordance with the terms of this Contract.

A determination by USARIEM that the Contractor has violated any of the information confidentiality and security provisions of this contract shall be a basis for USARIEM to terminate the contract for cause."

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object.

The TAIHOD does not collect data directly from individuals.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☐ **Yes** ☒ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

The TAIHOD does not collect data directly from individuals.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐	**Privacy Act Statement**	☐	**Privacy Advisory**
☐	**Other**	☒	**None**

Describe each applicable format.	The TAIHOD does not collect data directly from individuals.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.